TIFFANY CHEUNG (CA SBN 211497)
TCheung@mofo.com
DANIELLE VALLONE (CA SBN 302497)
DVallone@mofo.com
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105
Telephone: 415.268.7000
Facsimile: 415.268.7522

PURVI G. PATEL (CA SBN 270702)
PPatel@mofo.com
WENDY J. RAY (CA SBN 226269)
WRay@mofo.com
ERIK MANUKYAN (CA SBN 340307)
EManukyan@mofo.com
MORRISON & FOERSTER LLP
707 Wilshire Boulevard, Suite 6000
Los Angeles, California 90017
Telephone: 213.892.5200
Facsimile: 213.892.5454

Attorneys for Defendant
ORACLE AMERICA, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MICHAEL KATZ-LACABE, et al.,

Plaintiffs,

v.

ORACLE AMERICA, INC., a corporation organized under the laws of the State of Delaware,

Defendant.

Case No. 3-22-cv-04792-RS

DEFENDANT ORACLE AMERICA, INC.'S REPLY IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFFS' COMPLAINT, OR ALTERNATIVELY STRIKE PORTIONS OF THE COMPLAINT

Judge: Hon. Richard Seeborg

Date: February 9, 2023
Time: 1:30 p.m.
Courtroom: 3

Date Action Filed: August 19, 2022
Trial Date: Not set

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes & Rules

Other Authorities

Plaintiffs misread applicable law, mistake the prolix nature of their Complaint for plausibility, and ignore Oracle's actual statements (which the Court can consider through judicial notice) when inconvenient for their narrative. More critically, Plaintiffs ignore the laws under which Oracle is operating lawfully[1] and allege instead that Oracle's actions are unlawful under privacy laws they wished existed. But Plaintiffs cannot rely on their subjective hopes for what the law should be to expand it. Their claims fail as a matter of law for several reasons.

First, Plaintiffs' standing arguments are meritless; their cases are distinguishable and their claim that Oracle "conjures" third parties to defeat traceability is rebutted by the Complaint. ***Second***, non-California Plaintiffs' efforts to apply California law extraterritorially fail, and there is no basis to defer a choice-of-law ruling so they can seek irrelevant discovery from Oracle. Oracle's former California headquarters do not alter the analysis because the alleged conduct at issue occurred in Florida and Ireland. ***Third***, a review of even just a handful of the documents that Plaintiffs rely on in their Complaint demonstrate that they have failed to state a plausible privacy claim. Plaintiffs try to shoehorn Oracle's alleged conduct to the facts of *Facebook Tracking*, *Rodriguez*, and *Revitch*, but omit key distinctions that require dismissal of their privacy and CIPA/ECPA claims. As a result, their derivative UCL and declaratory judgment claims also fail. ***Finally***, Plaintiffs' equitable claims cannot proceed because they have an adequate remedy at law. The Court should thus dismiss the Complaint with prejudice.

I. ARGUMENT

A. Plaintiffs Lack Article III Standing

1. Plaintiffs fail to allege the requisite injuries

Largely relying on *TransUnion*, *Facebook Tracking*, and *In re Google RTB Consumer Priv. Litig.*, Plaintiffs argue that they have alleged "concrete and particularized" injury because those cases involved claims "substantively identical to the ones alleged here." (ECF No. 30 ("Opp.") at 3-4.) None of these cases support finding standing here.

[1] For example, Plaintiffs allege that Oracle is registered as a data broker in California and that it acts unlawfully when it acts as a data broker to help customers deliver relevant advertising to consumers in a manner that respects their privacy. They do not, however, allege that Oracle violates California's data broker law. Cal. Civ. Code § 1798.99.80.

First, *TransUnion LLC v. Ramirez* underscores that Plaintiffs' vague and speculative allegations, which rely on inferences of future harm, are insufficient to confer Article III standing. 141 S. Ct. 2190, 2211-13 (2021) ("risk of future harm, standing alone, cannot qualify as a concrete harm"). The *TransUnion* plaintiffs—who alleged only that the defendant *could have* divulged their information—did not suffer a concrete injury sufficient for standing. *Id.* Plaintiffs make similar speculative allegations about Oracle's and other data brokers' future actions. (*See*, *e.g.*, ECF No. 1 ("Compl.") ¶ 76 (speculative fears about information data brokers sell to the Chinese government), ¶ 80 (alleging Oracle *may* compile personal information from Planned Parenthood's website and *may* make it available to law enforcement).)

Second, the plaintiffs in *Facebook Tracking* alleged Facebook misrepresented that it would not collect data after users logged out and that it shared that information with seven million other websites. *See In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 596 (9th Cir. 2020), *cert. denied sub nom. Facebook, Inc. v. Davis,* 141 S. Ct. 1684 (2021) ("*Facebook Tracking*").[2] Plaintiffs do not and cannot allege here that Oracle made any such misrepresentations. Nor do they allege, as *Facebook Tracking* requires, a particularized injury that affects them in a "personal and individual way." *Id*. at 598 (citation omitted). They cite to generalized allegations about the conduct of data brokers (Compl. ¶¶ 24, 64, 74, 76) and assertions about how Oracle's products operate (*id.* ¶¶ 1, 45, 62, 65), but they fail to plausibly allege that Oracle sold or disclosed *their* data, causing *them* harm. And while Katz-Lacabe and Golbeck allege receiving documents "indicating Oracle had tracked, compiled, and analyzed" their data (*id.* ¶¶ 4, 6),[3] their "inference" that Oracle must have sold their data, causing harm, is speculation. (Opp. at 5.)

Third, the plaintiffs in *In re Google RTB Consumer Privacy Litigation* pled their alleged harms with far more particularity than Plaintiffs do here. 2022 WL 2165489, at *4 (N.D. Cal. June 13, 2022). In finding standing, the court relied on allegations specific to the plaintiffs,

[2] The same is true for *Campbell v. Facebook, Inc.*, 951 F.3d 1106, 1112 (9th Cir. 2020) where the plaintiff alleged Facebook shared sensitive private messages despite representing otherwise.

[3] Oracle is required to provide these "documents," which show the information collected and stored about an individual, upon request, under the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR). Cal. Civ. Code § 1798.130(a); GDPR Art. 15.

including their status as Google account holders and the platforms, web browsers, and user actions at issue, allowing the court to "draw a reasonable inference that [plaintiffs] have been injured by Google's conduct." *Id.*; *see also Al-Ahmed v. Twitter, Inc.*, 2022 WL 1605673, at *8 (N.D. Cal. May 20, 2022) (finding standing where plaintiff alleged he was *specifically* targeted and his private information was disclosed). In contrast, Plaintiffs fail to allege a single website they visited, what specific information about them Oracle purportedly collected or sold, or how Oracle harmed "their autonomy and their ability to control dissemination and use of information about them." (Compl. ¶ 117.)

Finally, the fact that courts have found standing for intrusion upon seclusion, CIPA, and federal Wiretap Act claims under different facts and circumstances (*see* Opp. at 3-5, and discussion above), does not mean that the Court should do so here. Moreover, the allegations Plaintiffs rely on to argue they have pled *current* harm (*id.* at 4 n.2), are too conclusory to allege injury. Their vague allegation that Oracle's conduct abrogates their autonomy, without more, fails to establish standing. *Spokeo, Inc. v. Robins,* 578 U.S. 330, 338-39 (2016) ("[T]he plaintiff must clearly . . . allege facts demonstrating each element [of standing]" (citation omitted)). Their remaining allegations concern potential future harms, which are too "conjectural or hypothetical" to confer standing. *Id.* at 339 (citation omitted); (*see*, *e.g.*, Compl. ¶¶ 73, 76, 82, 107, 117, 131).[4]

2. Plaintiffs fail to allege their injuries are traceable to Oracle's conduct

Plaintiffs are wrong that Oracle "conjures" third parties to break the causal links between Plaintiffs and Oracle for several reasons. (Opp. at 5.) First, they admit that there is no direct link between Oracle and Plaintiffs because they admit that Oracle has no direct relationship to Plaintiffs. (Compl. ¶¶ 1, 24, 86, 88, 91.) Second, Plaintiffs themselves identify the supposedly "conjured" third parties with whom they have relationships in the Complaint. (*Id.* ¶¶ 38, 41, 43 (alleging that numerous third-party website operators *chose* to deploy Oracle's code on their websites and collect consumers' personal information).)[5] Moreover, Plaintiffs have failed to

[4] Plaintiffs do not address, and therefore concede, Oracle's argument that they have not adequately pled future harm. *Yee v. Select Portfolio, Inc.*, 2018 WL 6173886, at *6 (N.D. Cal. Nov. 26, 2018) (Where a plaintiff fails to oppose a defendant's arguments in favor of dismissing a claim, the plaintiff has abandoned that claim.).

[5] Plaintiffs' reliance on *Revitch v. New Moosejaw*, 2019 WL 5485330 (N.D. Cal. Oct. 23,

demonstrate why these third parties with whom Plaintiffs admittedly interact ***do not*** break the purported causal chain with Oracle. *Cal. Advocs. for Nursing Home Reform, Inc. v. Chapman*, 2013 WL 5946940, at *7 (N.D. Cal. Nov. 5, 2013), *amended by* 2014 WL 2450949 (N.D. Cal. June 2, 2014).[6]

In terms of Oracle's alleged conduct, Plaintiffs concede that their claims are based on an "inference" that Oracle sells their data to third parties (Opp. at 5), but Plaintiffs cannot rely on "overly speculative" allegations that "rest on an attenuated chain of possibilities." *Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 681-82 (N.D. Cal. 2021) (dismissing for lack of standing where plaintiffs made "conclusory" allegations that Apple intercepted and disclosed their communications). Their generalized tracking and profiling allegations fare no better, as the nearly 50 paragraphs of the Complaint they cite in their opposition fail to contain a single allegation about Plaintiffs specifically. (*See* Opp. at 5 (citing Compl. ¶¶ 26-73).)

B. California Law Does Not Apply to Plaintiffs Golbeck and Ryan

1. The Court should not defer a choice-of-law analysis

Plaintiffs contend that the choice-of-law issues raised by Oracle are "premature" and "better addressed" at class certification because dismissing non-residents Golbeck and Ryan's claims without discovery would be "unduly prejudicial." (Opp. at 9.) But because the location of Oracle's headquarters and Plaintiffs' place of purported injury are known, there are no facts that could be located during discovery that could alter the Court's analysis. Plaintiffs tellingly fail to identify a single additional fact that could be relevant to the Court's decision on this issue.[7] *See Bartel v. Tokyo Elec. Power Co.*, 371 F. Supp. 3d 769, 790 (S.D. Cal. 2019) ("[A] choice-of-law analysis at the motion-to-dismiss stage" "is appropriate" so long as "discovery will not likely

---

2019) is misplaced. (Opp. at 5.) There, the court did not hold that third-party conduct is sufficient for traceability under Article III. *Revitch*, 2019 WL 5485330, at *2.

[6] Plaintiffs do not address or rebut this case, controlling authority on the issue. (ECF No. 23 ("Mot.") at 8.)

[7] *Swearingen v. Yucatan Foods, L.P.*, 24 F. Supp. 3d 889, 895 (N.D. Cal. 2014), *on reconsideration*, 59 F. Supp. 3d 961 (N.D. Cal. 2014), is distinguishable because it involved the "home state" exception to jurisdiction under the Class Action Fairness Act. Plaintiffs' remaining authority does not discuss discovery as a bar to a choice-of-law ruling at the pleading stage. *See Cullen v. Shutterfly Lifetouch LLC*, 2021 WL 2000247, at *9 (N.D. Cal. May 19, 2021); *Wallace v. SharkNinja Operating, LLC*, 2020 WL 1139649, at *15 (N.D. Cal. Mar. 9, 2020).

affect the analysis."). Without gaps in the relevant facts, discovery is not necessary to confirm the material differences in laws at issue, which is one reason courts have not deferred the choice-of-law decision. *See Potter v. Chevron Prods. Co.*, 2018 WL 4053448, at *10 (N.D. Cal. Aug. 24, 2018) (further development of the factual record unlikely to "materially impact the choice of law" analysis where plaintiffs were non-California residents allegedly injured out-of-state and defendant was headquartered in-state).

Moreover, courts in this district regularly consider extraterritoriality challenges at the pleading stage. "[T]he principle articulated in *Mazza* . . . is instructive even when addressing a motion to dismiss." *Frezza v. Google Inc.*, 2013 WL 1736788, at *5-8 (N.D. Cal. Apr. 22, 2013); *see also Cooper v. Tokyo Elec. Power Co. Holdings, Inc*., 960 F.3d 549, 557 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 1735 (2021) (it was not premature to decide choice of law questions on a motion to dismiss). The Court should not defer a ruling here.

2. Oracle has shown material differences among the applicable laws

Plaintiffs are simply wrong that Oracle points to "superficial differences" and "ma[kes] general references" in its analysis of Florida and European law. (Opp. at 8.) To the contrary, Oracle discusses these laws under the rubric of each prong of California's governmental interest test. (Mot. at 10-11.) Plaintiffs, in contrast, present little to rebut Oracle's showing.

With respect to Florida, they argue that "neither of the cases Oracle relies upon" in differentiating California's and Florida's intrusion upon seclusion tort "are like this one," which is precisely the point. (Opp. at 8 n.6.) While California law allows for certain claims premised on the collection of online data, Florida's laws have not stretched to reach any such claims. Indeed, Oracle is not aware of a single reported case like this one that has succeeded under Florida's intrusion upon seclusion tort.[8] With respect to the E.U., Plaintiffs contend many of the

[8] *See, e.g.*, *Malverty v. Equifax Info. Servs., LLC*, 407 F. Supp. 3d 1257, 1266-67 (M.D. Fla. 2019) (denying invasion of privacy claim based on intrusion upon seclusion and disclosure of private facts where Equifax allegedly disseminated plaintiff's credit report with data such as her social security number); *see also* Alex Pearce, *Time for a National Privacy Law?*, 38-SPG Del. Law. 6 (2020) (privacy laws across the 50 states are a "fragmented patchwork").

Moreover, Florida's decision not to pass a consumer privacy law conferring substantive data privacy rights to its citizens is a "policy choice[]" separate from California that should be respected. *Mazza v. Am. Honda Motor Co.*, 666 F.3d 581, 591 (9th Cir. 2012); *compare* H.B. 9, 2022 Fla. Leg., Reg. Sess. (Fla. 2022) (unenacted) *and* S.B. 1864, 2022 Fla. Leg., Reg. Sess. (Fla.

"substantive data protection rights under the GDPR [] mirror those available under California law" (Opp. at 8-9), but they do not identify or analyze any comparative law.[9]

Next, contrary to Plaintiffs' argument (Opp. at 9), Oracle also addressed the remaining two prongs of California's governmental interest test. As Oracle discussed (Mot. at 10-11), a true conflict exists because the boundaries of digital privacy are prescribed by the community, and Florida and the E.U. have the "predominant interest" in applying their own laws as "the place of the wrong." *Stromberg v. Qualcomm Inc.*, 14 F.4th 1059, 1070 (9th Cir. 2021) (vacating class certification on choice of law grounds) (citation omitted); *see also Hillard v. TABC, Inc.*, 2017 WL 6940540, at *6 (C.D. Cal. Dec. 18, 2017) (the Texas legislature's consumer protection policy concerns trumped California's interest in regulating companies headquartered within its borders).

3. Plaintiffs' allegations of misconduct in California are inadequate

Plaintiffs do not meaningfully address Oracle's argument that the place of the wrong is ***not*** California, instead arguing that California law should apply to non-resident Plaintiffs' claims because the alleged misconduct emanated from the state. *Stromberg*, 14 F.4th at 1073 (the place of the wrong is "where the last event necessary to make the actor liable occurred" (citation omitted)); (Opp. at 7-8). This level of contact, however, was insufficient in *Mazza*, and for the same reasons, is insufficient here. 666 F.3d at 590 (district court erred in applying California law nationwide even though the defendant's headquarters and the advertising agency responsible for the alleged misrepresentations were located in the state). The contact is also insufficient to extend the UCL beyond California's borders. (Opp. at 7; *see also* Compl. ¶¶ 10, 15, 16.) Despite Plaintiffs' argument to the contrary, courts have repeatedly found that a defendant's base of operations is irrelevant when the alleged conduct at issue occurred outside of California.[10] *See*,

---

2022) (unenacted) *with* Cal. Civ. Code §§ 1798.100, *et seq.* (detailing the several data privacy rights conferred to California consumers under the California Privacy Rights Act).

[9] The GDPR's comprehensive privacy framework diverges from intrusion upon seclusion under California law because it provides clear boundaries for what is lawful and unlawful, prescribing conduct regarding opt-ins, opt-outs, and erasure, all the while delineating rights, such as the right to restrict data processing, that are absent from the common law claim. *See* GDPR Art. 4 (defining the boundaries of consent, proper opt-ins, and proper opt-outs); *see also id.* at Chapter 3 (detailing the various rights of the Data Subject).

[10] Plaintiffs' cases do not warrant a different result. Because the "decisions" to place JavaScript code or cookies on websites were made by Oracle's customers, Plaintiffs' argument that Oracle is headquartered in California is insufficient to demonstrate that the purported

e.g., *Sullivan v. Oracle Corp.*, 51 Cal. 4th 1191, 1208 (2011) (focusing inquiry on where the payment or underpayment actually occurred, rather than Oracle's headquarters); *see also Frezza*, 2013 WL 1736788, at *5 (dismissing foreign plaintiffs' UCL claims where the defendant was headquartered in California, but the transactions at issue occurred in North Carolina)*; see also Allergan USA Inc. v. Imprimis Pharms., Inc.*, 2019 WL 3029114, at *8 (C.D. Cal. July 11, 2019) (rejecting argument that the UCL should block out-of-state drug transactions because "the conduct giving rise to liability occurs at Defendant's headquarters in California"). The same result is warranted here.

C. The Complaint Fails to State a Claim Under Rule 12(b)(6)

Contrary to Plaintiffs' argument (Opp. at 1), Oracle relies on the same documents that Plaintiffs cite to and rely on for their allegations against Oracle (*cf.* ECF No. 23-1 ("Patel Decl.") Exs. A-L, *with*, *e.g.*, Compl. ¶¶ 22, 29, 32-33, 36, 39-40, 42-43). The law does not allow Plaintiffs to cherry pick. *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1002 (9th Cir. 2018) (the incorporation-by-reference doctrine prevents plaintiffs from selecting only the portions of documents that support their claims and omitting portions that weaken them).

1. Plaintiffs fall far short of Rule 8's pleading standards

Rather than help Plaintiffs, their "extensive allegations and factual citations" (Opp. at 9) violate Rule 8's requirement for "a *short and plain* statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2) (emphasis added). Critically, the Complaint is rife with allegations about Oracle's purported conduct (Opp. at 10), but Plaintiffs do not allege how that conduct has harmed *them specifically*, making essentially an "unadorned, the-defendant-unlawfully-harmed-me accusation." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

Plaintiffs also wrongly claim that their redundant and immaterial allegations should not be stricken because they "directly relate to Oracle's conduct." (Opp. at 10.) Even a cursory review

---

misconduct occurred in California. *See Collazo v. Wen by Chaz Dean, Inc.*, 2015 WL 4398559, at *3 (C.D. Cal. July 17, 2015) (focusing analysis on "where decisions regarding WEN's product ingredients and product advertisements—the alleged misconduct in [that] case—occurred"); *see also Fernandez v. CoreLogic Credco, LLC*, 593 F. Supp. 3d 974, 989 (S.D. Cal. 2022) (finding that a decision was premature due to insufficient information as to where the disputed "final act" occurred). And in *Stromberg*, the court did not evaluate the extraterritorial application of the UCL, rendering it inapposite. 14 F.4th at 1073.

of the allegations shows that they are not related to Oracle at all:

- Paragraphs 76-79 and 81 involve statements about data brokers generally in relation to unpassed Congressional bills and do not reference Oracle at all.
- Paragraphs 64-65 and 80 allege that Oracle *can* "traffic" in individuals' "highly sensitive personal information," a claim that is not about what Oracle actually does.
- Paragraph 147 vaguely identifies a purported exposure of a server holding BlueKai records from over two years ago but does not allege that it impacted Plaintiffs.

Plaintiffs also suggest that Oracle seeks to strike these allegations because they are "embarrass[ing]." (*See id.*) Not so. Oracle seeks to strike these paragraphs because they have no bearing on Plaintiffs' claims. Fed. R. Civ. P. 12(f); *see Ho v. Pinsukanjana*, 2018 WL 2425980, at *3 (N.D. Cal. Apr. 24, 2018).

2. Plaintiffs' privacy claims fail (first and second causes of action)

a. Plaintiffs lack a reasonable expectation of privacy

Plaintiffs argue that because they allege that Oracle collects their online and offline activity[11] and compiles it into a "vast repository of personal data" (Opp. at 11), they have alleged a reasonable expectation of privacy. Though they recite the legal standard, they do not assess the "variety of factors" courts consider, "including the customs, practices, and circumstances surrounding a defendant's particular activities." *Facebook Tracking*, 956 F.3d at 601-02. Critical to this analysis is (i) the "nature" or "manner" of collection and (ii) the "sensitivity" of the data. *Id.* at 603. Plaintiffs' allegations do not satisfy these factors.

At issue here is data that Oracle collected on behalf of its customers, with their consent. Plaintiffs admit they are not in privity with Oracle (Opp. at 12), and that difference alone makes their reliance on *Facebook Tracking*—where the plaintiffs ***were*** in privity with Facebook—inapposite. (*Id.* at 11). Further, in that case the Ninth Circuit repeatedly noted that "the relevant question" was "whether a user would reasonably expect that Facebook would have access to the user's individual data ***after the user logged out of the application.***" *Facebook Tracking*, 956 F.3d at 602 (emphasis added). This fact was crucial to the court's analysis, as well as subsequent courts that have also considered claims for an invasion of privacy or intrusion upon

[11] Plaintiffs' allegations of offline activities are limited to activities "including their brick-and-mortar purchases and location information." (Compl. ¶¶ 115-16, 129-30.)

seclusion based on the alleged collection of consumer information. *Id.*; *Rodriguez v. Google LLC*, 2021 WL 2026726, at *8 (N.D. Cal. May 21, 2021);[12] *Brown v. Google LLC*, 2021 WL 6064009, at *1 (N.D. Cal. Dec. 22, 2021) (finding that Google was tracking data in "Incognito Mode" in Chrome). Plaintiffs do not, and cannot, allege that Oracle failed to adhere to its own policies and do not cite any authority for their attempted expansion of the law. Nor do they cite any misrepresentations by Oracle's customers regarding third-party data collection, which cannot be laid at Oracle's door in any event.

Moreover, unable to support a claim that browsing history data, app usage data, contact information, home location, and device data are sensitive on an individual basis (Compl. ¶¶ 27, 44, 49, 164), Plaintiffs instead argue that the data is sensitive *in aggregate*. (Opp. at 13.) But their only cited case for this point, *In re Google Location History Litigation*, has limited utility outside the "location data" context. 514 F. Supp. 3d 1147, 1157 (N.D. Cal. 2021). There, the court analogized Google's conduct to the "continual GPS tracking" that supported invasions of privacy in two criminal cases involving law enforcement's use of (i) a GPS tracking device placed underneath a car and (ii) location data from cell towers. *Id.* (citing *United States v. Jones*, 565 U.S. 400, 417 (2012) and *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018)).

Plaintiffs' conclusory allegations that Oracle generally collects health, biometric, genetic, pregnancy, religion, political, or sexual orientation information (*see*, *e.g.*, Compl. ¶¶ 82, 114) fare no better. While they "devote many pages" to describing political, racial, or medical data (Opp. at 13), they erroneously conflate the conduct of *other* data brokers with Oracle's conduct (Compl. ¶¶ 63-65 (discussing allegedly problematic types of data that Mobilewalla, Acxiom, and Gravy Analytics collect without any plausible basis to conclude that Oracle does the same or that it acquires such data from those other third parties)). Further, there is no allegation that Oracle specifically collected the ***named Plaintiffs'*** biometric, genetic, pregnancy, religion, political, or sexual orientation data, further demonstrating the conclusory nature of their allegations.

[12] Plaintiffs cite *Rodriguez* but fail to discuss the totality of considerations this Court found important. (Opp. at 13-14.) The Court emphasized *both* the manner (or nature) of collection and the sensitivity of the data, and stressed Google's collection of browsing habits after it had "set an expectation" it would not do so. *Rodriguez*, 2021 WL 2026726, *8 (citation omitted).

b. Oracle's conduct is not "highly offensive" or "egregious"

Courts regularly resolve whether conduct is "highly offensive" or "egregious" at the pleading stage where, as here, the alleged data collection practices constitute "routine commercial behavior."[13] (Opp. at 14); *see Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011), *modified*, June 7, 2011 (sustaining demurrer as to the invasion of privacy claim); *see also Hammerling v. Google LLC*, 2022 WL 2812188, at *11-12 (N.D. Cal. July 18, 2022) (dismissing invasion of privacy claims finding conduct not "highly offensive" or "egregious"). Further, given Plaintiffs' allegation that Oracle is a registered "data broker" under California law, it follows that Oracle collects data from individuals with whom it "does not have a relationship." Cal. Civ. Code § 1798.99.80; (Compl. ¶¶ 10, 24, 74). Under this law, Oracle's alleged conduct constitutes the "routine commercial behavior" of a registered data broker.

Even so, Plaintiffs argue that their invasion of privacy claim should not be dismissed because Oracle is the only party privy to the "true extent" of its privacy intrusion. (Opp. at 14 (citing *Hayden v. Retail Equation*, 2022 WL 2254461 (C.D. Cal. May 4, 2022)).) But *Hayden* does not help. There, the court found the plaintiffs alleged facts that were "more nefarious than the mere collection of routine information," including the collection of consumers' photographs. *Id.* at *8. Plaintiffs do not (and cannot) meet that threshold, as they do not allege that Oracle has failed to comply with any obligations under the California Civil Code applicable to data brokers. Rather, they rely on conclusory allegations that Oracle engages in more than "routine commercial behavior," citing selectively to articles that mention Oracle while criticizing the purported "surveillance" practices of the advertising technology industry generally. (Opp. at 16.)

Plaintiffs also try, and fail, to use select testimonials about the malevolence of data brokers to support their contention that Oracle's conduct violates community norms. Plaintiffs

[13] *Williams v. Facebook, Inc.* and *Facebook Tracking* are distinguishable. 384 F. Supp. 3d 1043, 1055 (N.D. Cal. 2018); 956 F.3d at 606. In *Williams*, this Court determined that whether Facebook's conduct was egregious or merely "routine commercial behavior" was a question of fact given plaintiffs allegations of "lack of any advance notice or opportunity to consent." 384 F. Supp. at 1055 (citation omitted). And, as discussed, in *Facebook Tracking,* the Ninth Circuit found the allegations of offensiveness enough to "survive a Rule 12(b)(6) motion to dismiss" based in part on allegations "of surreptitious data collection when individuals were not using Facebook." 956 F.3d at 606.

point to unidentified actions in Europe and the U.K. against Oracle—neither of which represent community norms in this country, let alone California—and Federal Trade Commission warnings about data brokers generally. (*Id.*; Compl. ¶ 118.) Likewise, their attempt to use the opinions of two U.S. Senators from Oregon and Massachusetts to define community norms in California, or even the entire nation, is untenable. *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal.4th 1, 37 (1994) (holding that a "reasonable" expectation of privacy must be "relative to the customs of the time and the place"); (*see also* Opp. at 15-16; Compl. ¶¶ 76, 78, 81, 119, 133). Thus, Plaintiffs have failed to plausibly allege any highly offensive conduct or an egregious breach of social norms.

3. Plaintiffs have not stated a UCL claim (third cause of action)

Plaintiffs argue based on two distinguishable cases that they have alleged an economic injury, and thus standing, under the UCL. (Opp. at 20-21.) The *Brown* court held that the plaintiffs had adequately pled a loss of money or property because they identified, ***with specificity***, the economic value of their personal information. 2021 WL 6064009, at *15 (plaintiffs quantified data value based on platforms that compensate consumers for the use of their data).[14] Plaintiffs have not pled any such facts here. *Calhoun v. Google LLC*, 526 F. Supp. 3d 605 (N.D. Cal. 2021) is also distinguishable; it relies on data breach cases pleading benefit-of-the-bargain losses stemming from a breach of contract. (*See* Opp. at 21 (citing same cases).)

Plaintiffs add little to address whether they satisfy either the unlawful or unfair prong of the UCL.[15] The parties agree that if Plaintiffs fail to properly allege a violation of a predicate law, their "unlawful" claim fails. (*Id.* at 21-22.) With respect to the "unfair" claim, Plaintiffs contend they satisfy both the balancing and tethering tests. But for the balancing test, they do not identify a single allegation that shows "the harm [purportedly] caused by the unauthorized collection and dissemination of Plaintiffs' personal information clearly outweighs the utility of that sale." (*Id.* at 22.) As for the tethering test, Plaintiffs argue that "numerous California

[14] *Klein v. Facebook, Inc.* (Opp. at 20) cites *Brown*, but it addressed economic injury for antitrust claims, not the UCL. 580 F. Supp. 3d 743, 804 (N.D. Cal. 2022).

[15] Plaintiffs fail to address, and therefore concede, Oracle's argument that because the alleged unfair business practices overlap entirely with the alleged unlawful business practices, the unfair claim cannot survive if the unlawful one does not. (Mot. at 22); *Yee*, 2018 WL 6173886, at *6.

statutes, including the CCPA, reflect California's public policy of protecting consumer data."[16] (Opp. at 22 (citation omitted).) Again, Plaintiffs do not cite a single allegation in the Complaint that tethers Oracle's allegedly unfair practices with the CCPA (or any of the other "numerous" statutes). Rather than tying Oracle's conduct to a "legislatively declared policy" as required (Mot. at 23), Plaintiffs attempt to tether Oracle's conduct to proposed—but unpassed—legislation (*see, e.g.*, Compl. ¶¶ 63, 74, 76-79, 81, 112, 126). That is insufficient under the law.

4. Plaintiffs' wiretapping claims fail (fourth and fifth causes of action)

Plaintiffs do not dispute, and therefore concede, that their CIPA and ECPA claims fail because (1) the Wiretap Act is a one-party consent statute and Oracle's customers have consented, (2) Plaintiffs fail to state a CIPA § 631(a)(iii) claim, and (3) Plaintiffs fail to state a CIPA § 631(a)(iv) claim. The arguments Plaintiffs do make fail for three independent reasons.

Oracle is a party to Plaintiffs' communications. Oracle deploys its bk-coretag.js code only when permitted by its customers, and solely as a service provider for the customers' benefit. As such, Oracle is a mere "extension" of its customers rather than a third-party eavesdropper. *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 832 (N.D. Cal. 2021) (exempting a service provider from wiretapping liability as a party to the communication). Plaintiffs rely on *Facebook Tracking* and *Revitch*, but they are clearly distinguishable. There, other independent data companies allegedly "mined information from other websites." *Id*. Plaintiffs make no such mining allegation here.[17] In *Facebook Tracking*, the court also found that Facebook's conduct was unauthorized based on allegations it tracked users ***after*** they had logged out of Facebook, despite its representations that it would not do so. 956 F.3d at 598-99. And in *Revitch*, the plaintiff sufficiently alleged that NaviStone secretly scanned his computer for files that could be used to de-anonymize and identify him. 2019 WL 5485330, at *1; (ECF No. 43 ("SAC") ¶ 3). Plaintiffs

[16] Plaintiffs do not and cannot assert CCPA claims. And they are wrong to argue that Oracle's conduct violates the CCPA. (Opp. at 22.) The CCPA does not regulate cookies or require consumer consent; rather, it can impact use of certain types of cookies ***if*** the company engages in certain online advertising via cookies, which could constitute a "sale" under the Act. Cal. Civ. Code § 1798.100, *et al*. Plaintiffs seek to use this Court as an end run around the California legislature in asking it to impose requirements above and beyond the CCPA.

[17] Plaintiffs' claim that Oracle mined data via the bk-coretag.js is unsupported by the Complaint. Plaintiffs cannot attempt to amend their Complaint via their opposition brief. (Opp. at 18); *see Tietsworth v. Sears*, 720 F. Supp. 2d 1123 (2010).

do not allege that Oracle scans their computers for files that can be used to identify them or that it de-anonymizes their data; rather, they allege that Oracle's customers use bk-coretag.js to analyze their own data, target their own advertisements, and measure their own advertising reach. (*See* Compl. ¶ 30 n.15 (describing how *customers* can use collected "coretags" to organize visitor data); *see also* Patel Decl. Ex. D.)

Oracle did not intercept the "contents" of Plaintiffs' communications. Plaintiffs allege Oracle's bk-coretag.js code captured (i) referrer URLs; (ii) webpage titles; (iii) webpage keywords; (iv) date and times of website visits; (v) IP addresses; (vi) page visits; (vii) purchase intent signals; (viii) add to cart action; and (ix) data entered into forms. (Compl. ¶¶ 32, 164.) They do not substantively contest and thus concede that categories (ii)-(viii) are non-content record information. (Opp. at 18-19); *see also Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1082-83 (C.D. Cal. 2021) (IP addresses, shipping/billing information, visit date/time, page views, and website movements are not "content"); *Svenson v. Google Inc.*, 2015 WL 1503429, at *7 (N.D. Cal. Apr. 1, 2015) (finding same based on *Zynga*).

Plaintiffs' argument that referrer URLs and entries to forms are content (Opp. 18-19), are too conclusory to state a claim. In contrast to the cases Plaintiffs cite, Plaintiffs allege only that Oracle intercepted the "contents" of Plaintiffs' URLs, without specifying whether the referrer headers contained "search terms" or "basic identification and address information." *See In re Zynga Priv. Litig.*, 750 F.3d at 1107-09 (9th Cir. 2014) (dismissing wiretapping claims on allegations of the latter).[18] Plaintiffs' allegations about entries to an online form are similarly unhelpful. Contrary to Plaintiffs' reading, neither *Zynga* nor *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir. 2003) hold that all entries into a web form are "content." *Zynga*, 750 F.3d at 1107. In evaluating *Pharmatrak*, the Ninth Circuit reached a far narrower conclusion: because users had

[18] Plaintiffs' cases are consistent with *Zynga*. *See In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 138-39 (3rd Cir. 2015) (in view of *Zynga*, "some queried URLs qualify as content"); *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 275 (3d Cir. 2016) (Google intercepted content where Viacom allegedly permitted Google to access URLs revealing the videos a child watched); *In re Google RTB Consumer Priv. Litig.*, 2022 WL 2165489, at *10 (N.D. Cal. June 13, 2022) (court did not specifically identify URL impressions as content). Despite what Plaintiffs contend, *Facebook Tracking* did not address whether a URL constituted "content" under CIPA or ECPA. 956 F.3d at 607.

entered ***their personal medical information*** into a webform, the First Circuit concluded that the defendant disclosed the contents of a communication. *Id*. Here, Plaintiffs have not alleged that they typed any information into a webform, let alone sensitive information.

The Wiretap Act's crime-tort exception is inapplicable. Plaintiffs concede that Oracle's customers consented to Oracle's participation in Plaintiffs' alleged communications. (Opp. at 19-20.) To avoid dismissal, they assert their communications were intercepted to commit a criminal or tortious act. (*Id*.) For this exception to apply, Plaintiffs must allege that the primary motivation or a determining factor in Oracle's actions was to injure Plaintiffs tortiously. *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1067 (N.D. Cal. 2021). They have not. They instead argue, without support, that Oracle intercepted their communications for the secondary independent purpose of committing tortious acts. (Opp. at 20.) Courts in this district—including this Court—have found that the crime-tort exception is inapplicable where the defendant's primary motivation was to make money. *Rodriguez*, 2021 WL 2026726, at *6 n.8; *In re Google Inc. Gmail Litig.*, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014). Plaintiffs cannot plausibly allege that Oracle's primary motivation was not financial.

5. Plaintiffs' unjust enrichment claim fails (sixth cause of action)

Plaintiffs argue that unjust enrichment is a standalone claim and that *Astiana v. Hain Celestial Grp., Inc.,* 783 F.3d 753 (9th Cir. 2015) no longer governs based on an unpublished decision: *Brooks v. Thomson Reuters Corp.*, 2021 WL 3621837 (N.D. Cal. Aug. 16, 2021). But this and other courts have followed *Astiana* after *Brooks*. *See Davidson v. Sprout Foods Inc.*, 2022 WL 2668481, at *6 (N.D. Cal. July 11, 2022); *Crown Cell Inc. v. Ecovacs Robotics, Inc.*, 2022 WL 17082670, at *4 (N.D. Cal. Nov. 18, 2022) (same); *Sanchez v. Nurture, Inc.*, 2022 WL 4097337, at *8 (N.D. Cal. Sept. 7, 2022) (same). Plaintiffs cannot convert their claim into a quasi-contract claim for restitution because they have failed to allege (1) mistake, fraud, coercion, or request, and (2) that they conferred a benefit on Oracle that would be unjust to retain. (Mot. at 24.) They do not address the former and miss the mark on the latter. Rather than direct the Court to a single supportive allegation, Plaintiffs argue that they are not required to show a corresponding loss (Opp. at 23), an argument that Oracle does not make.

6. Plaintiffs are not entitled to equitable relief under *Sonner*

Plaintiffs' equitable and legal claims are based on the same wrongdoing and seek essentially the same remedies—restitution and disgorgement for the privacy claims, damages for the CIPA claim, and statutory damages for the Wiretap Act claim. (Compl. ¶¶ 123, 137, 157, 172.) They fail to allege that the legal remedies are inadequate. *Sonner v. Premier Nutrition Corp.*, 971 F.3d 834, 844 (9th Cir. 2020). Thus, their argument that they have pled remedies that "go beyond" damages is irrelevant. (Opp. at 24); *Hrapoff v. Hisamitsu Am., Inc.*, 2022 WL 2168076, at *6 (N.D. Cal. June 16, 2022) (failure to allege an inadequate remedy is fatal). So too is their argument that they seek "prospective" injunctive relief as they do not adequately allege what future harm would be prevented. (Opp. at 24); *Deitz v. Comcast Corp.*, 2006 WL 3782902, at *3 (N.D. Cal. Dec. 21, 2006).[19] Because Plaintiffs cannot sufficiently allege that they lack an adequate legal remedy, their equitable claims should be dismissed without leave to amend. *See In re MacBook Keyboard Litig.*, 2020 WL 6047253, at *4 (N.D. Cal. Oct. 13, 2020) (availability of an adequate legal remedy was clear from the face of the SAC so amendment would be futile).

7. Plaintiffs' declaratory judgment claim fails (seventh cause of action)

A declaratory judgment claim cannot stand where Plaintiffs have failed to state a claim based on any underlying law; therefore, because Plaintiffs have failed to allege facts sufficient to state a claim under any of the above referenced causes of action, this cause of action must be dismissed too. (*See* Opp. at 25; Mot. at 25.) Plaintiffs also do not contend, as they must, that this claim seeks anything beyond what they seek in their underlying claims. *Tech & Intellectual Prop. Strategies Grp. PC v. Fthenakis*, 2011 WL3501690, at *10 (N.D. Cal. Aug. 10, 2011).

II. CONCLUSION

Plaintiffs' opposition confirms that, despite their "extraordinarily detailed allegations" they have not and cannot state a claim.

[19] *Kellman v. Spokeo, Inc.* is inapposite; that case did not address pleading requirements under *Sonner*, 599 F. Supp. 3d 877, 897 (2022).

Dated: January 20, 2023

MORRISON & FOERSTER LLP

By: *Purvi G. Patel*
Purvi G. Patel

Attorneys for Defendant Oracle America, Inc.